REMARKS

Claims 1-3 and 5-10 are currently pending in the subject application, and are presently under consideration. Claims 1-3 and 5-10 are rejected. Favorable reconsideration of the application is requested in view of the comments herein.

I.   **Rejection of Claims 1-3 and 5-10 Under 35 U.S.C. §102(e)**

Claims 1-3 and 5-10 stand rejected under 35 U.S.C. §102(e) as being anticipated by U.S. Patent No. 5,922,074 to Richard, et al. ("Richard"). Withdrawal of this rejection is respectfully requested for at least the following reasons.

Claim 1 recites configuring a first directory with information regarding users with signature certificates associated with the second enterprise PKI that are allowed access to the server. Claim 1 also recites sending a query to a second directory from the first directory to determine if the user is a member of the second enterprise PKI, the second directory being part of the second enterprise PKI. The invention of the present application is advantageous in that it permits trusted communication across different PKI enterprises without having to authenticate a chain of trust from a certifying authority. The Office Action dated February 2, 2005, asserts that claim 1 is taught by Richard. Representative for Applicant respectfully disagrees.

Richard discloses a method and apparatus for providing a public key infrastructure via secure directory services within a computer system and/or a computer network (col. 1, ll. 10-13). A server receives a client identity from a directory client using an underlying secure communications protocol (col. 7, ll. 5-7). In Richard, client identity is determined in the following manner:

> Since servers and clients are issued identities (DN's) from some directory service
> before they participate in secure communications, they are able to at least identify
> their "home" directory service. Their "home" directory service communicates
> with other directory services, each "serving" their lists of electronic identities to
> each other using secure directory services. In this manner, a client or server can
> verify the peer identity of a secure communicator by relying on the trusted
> "home" directory service. (col. 3, ll. 30-40).

Assuming *arguendo* that each "home" directory service corresponds to a separate PKI enterprise, this passage demonstrates that Richard does not teach a first directory with information regarding users with signature certificates associated with the second enterprise PKI that are allowed access to the server, as recited in claim 1. This passage describes that each of the home directory services serves their lists of identities to each other using secure directory services. Richard expounds upon this by stating that, by securely receiving identity verification services from a directory service, the server can then determine the access rights to grant to a client, allowing a server to deliver client-sensitive information without prior knowledge of the client (col. 2, ll. 35-39). Thus, in the system of Richard, if the server does not have knowledge of a client (because it is from a different "home" directory service), it must receive identity verification from the other directory service. This does not correspond to storing information on a first directory regarding users with signature certificates associated with a second enterprise PKI that are allowed access to a server on the first enterprise PKI, as described in claim 1.

In addition, the following passage further describes the verification process taught by Richard:

> [T]he server checks if the client identity is recognized by the internal directory database. Thus, if directory client 40 transmits client identity information in the form of a digital certificate...server 42 checks the digital certificate to confirm recognition from its internal database....[I]f the internal directory database 50 has no information regarding the certificate's signer, the client will not be identifiable. Under such circumstances, the server may act as a client to retrieve the required signer's public key information from another server to complete the identification. Details of this process are described in further detail in conjunction with FIG. 6... (col. 7, ll. 50-64).

Thus, in the verification process taught by Richard, a first server must access a different server to access key information for a client wishing to obtain access to the server if no information exists for that client in the server's database. This further demonstrates that information regarding signature certificates associated with a PKI enterprise separate from the first server is not stored on the first server.

In addition, the Office Action dated February 2, 2005, asserts that Richard teaches configuring a first directory with information regarding users with signature certificates

associated with the second enterprise PKI that are allowed access to the server, as recited in claim 1, in FIG. 6A and 6B. Representative for applicant disagrees. The above cited passage (at col. 7, ll. 50-64) demonstrates that flowchart of FIG. 6 applies to the situation when a server may act as a client to retrieve the required signer's public key information from another server to complete the identification. This situation is, as demonstrated in the cited passage above, in response to not having information regarding the certificate's signer. Therefore, Richard does not teach, in neither FIGs. 6A and 6B nor anywhere else, configuring a first directory with information regarding users with signature certificates associated with the second enterprise PKI that are allowed access to the server, as recited in claim 1.

Even assuming *arguendo* that Richard teaches configuring a first directory with information regarding users with signature certificates associated with the second enterprise PKI that are allowed access to the server, as recited in claim 1, Richard still does not disclose each and every element of claim 1. The Office Action dated February 2, 2005, cites the above passage (page 3, citing Richard, col. 7, ll. 61-63) to assert that Richard teaches sending a query to a second directory from the first directory to determine if the user is a member of the second enterprise PKI, the second directory being part of the second enterprise PKI. It is respectfully submitted that this assertion is incorrect. The above passage from Richard specifically states that the server acts as a client to retrieve the required signer's public key information from another server to complete the identification in response to not having information regarding the certificate's signer. Therefore, having information regarding the certificate's signer and acting as a client to retrieve the required signer's public key information from another server to complete the identification are disclosed by Richard as mutually exclusive conditions. Accordingly, Richard does not teach both configuring a first directory with information regarding users with signature certificates associated with the second enterprise PKI that are allowed access to the server, and sending a query to a second directory from the first directory to determine if the user is a member of the second enterprise PKI, the second directory being part of the second enterprise PKI, as recited in claim 1. Additionally, in the capacity of acting as a client on another server, the system of Richard determines if the public key of the certificate issuer is valid

in order to obtain a chain of trust with the certifying authority that issued the client's certificate (see, *e.g.*, Richard, col. 9, line 54 through col. 10, line 46). This element is not necessary in the method described by claim 1, as trust has already been established with the user from the separate PKI enterprise because the first directory has been configured with information regarding users with signature certificates associated with the second enterprise PKI, and the first directory sends a query to a second directory associated with the second enterprise PKI to determine if the user is a member of the second enterprise PKI, as recited in claim 1 (see, *e.g.*, present application, paragraph 32).

For at least the reasons described above, Richard does not disclose each and every element of claim 1, and thus does not anticipate claim 1. Accordingly, withdrawal of the rejection of claim 1, as well as claims 2, 3, and 5 which depend therefrom, is respectfully requested.

Claim 6 recites a first directory that is part of a first enterprise PKI and including a directory entry that includes users with signature certificates from the second enterprise PKI that are allowed access to the server, and a query sent to the second directory from the first directory being sent to determine if at least one user is a member of the second enterprise PKI. For at least the reasons described above regarding claim 1, claim 6 is also not anticipated by Richard. Withdrawal of the rejection of claim 6, as well as claims 7-9 which depend therefrom, is respectfully requested.

Claim 10 recites receiving a query from a server requesting if a user is allowed access to the server, the server being part of the first enterprise PKI and including a directory entry including users with signature certificates from the second enterprise PKI that are allowed access to the server. Claim 10 also recites sending a query to the directory to determine if the user is a member of the second enterprise PKI, the directory being part of the second enterprise PKI. For at least the reasons described above regarding claim 1, claim 10 is also not anticipated by Richard. Withdrawal of the rejection of claim 10 is respectfully requested.

CONCLUSION

In view of the foregoing remarks, Applicant respectfully submits that the present application is in condition for allowance. Applicant respectfully requests reconsideration of this application and that the application be passed to issue.

Please charge any deficiency or credit any overpayment in the fees for this amendment to our Deposit Account No. 20-0090.

Respectfully submitted,

Date   3/29/05

Christopher P. Harris
Registration No. 43,660

CUSTOMER NO.: 26,294

TAROLLI, SUNDHEIM, COVELL, & TUMMINO L.L.P.
526 SUPERIOR AVENUE, SUITE 1111
CLEVELAND, OHIO 44114-1400
Phone: (216) 621-2234
Fax: (216) 621-4072